U.S. DEPARTMENT OF ENERGY
Office of Electricity Delivery and Energy Reliability

Electricity Sector Cybersecurity Risk Management Process Guideline
EXECUTIVE SUMMARY

Overview

The Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline was developed by the Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and representatives from both the public and private sectors. The primary goal of the guideline is to describe a risk management process that is targeted to the specific needs of electricity sector organizations. The NIST Special Publication 800-39, *Managing Information Security Risk* provides the foundational methodology of this document. The guideline adds to the body of resources that help refine the definition and application of effective cybersecurity for all organizations across the electricity sector. The RMP guideline is designed to build on an organization's existing cybersecurity program, policies and procedures, to help organize and clarify risk management goals, and to provide a consistent approach to make risk decisions.

Over the past few decades, the electricity sector has become increasingly dependent on digital technology to reduce costs, increase efficiency and maintain reliability during the generation, transmission and distribution of electric power. The information technology (IT) and industrial control systems (ICS) that utilize digital technology can be as vulnerable to malicious attacks and misuse as other types of communication systems. These vulnerabilities highlight the need for defense of the integrated power system, which requires constant vigilance and expertise. The role of managing cybersecurity risk, from the operation and use of IT and ICS, is critical to the success of organizations to achieve their strategic goals and objectives, including resiliency, reliability, and safety.

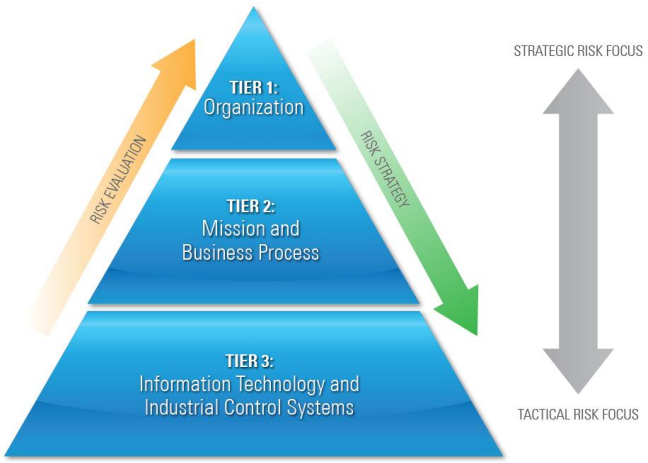
The successful application of this guideline will result in the ability of an electricity sector organization to:

- Effectively and efficiently implement a cybersecurity risk management process across the entire organization;
- Establish the organizational tolerance for risk and communicate it through the organization including guidance on how risk tolerance impacts risk decision making;
- Prioritize and allocate resources for managing cybersecurity risk;
- Create an organizational climate where cybersecurity risk is considered within the context of the mission and business objectives of the organization; and
- Improve understanding of cybersecurity risk and how these risks impact the mission and business success of the organization.

Risk Management Process

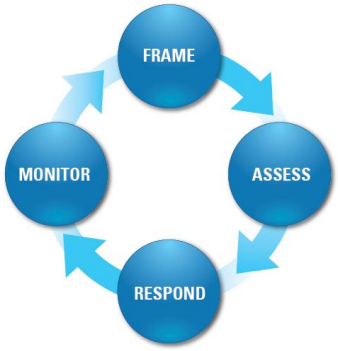
The risk management process explained in this guide has two primary components; the risk management model and the the risk management cycle. The risk management model reflects the organization as a three-tiered structure and provides a comprehensive view for the electricity sector organization and how risk management activities are undertaken across the organization. This structure is simple enough that it can be applied to any electricity sector organization regardless of size or operations. The three tiers of the risk management model are:

Tier 1: Organization
Tier 2: Mission and Business Process
Tier 3: Information Technology and Industrial Control Systems



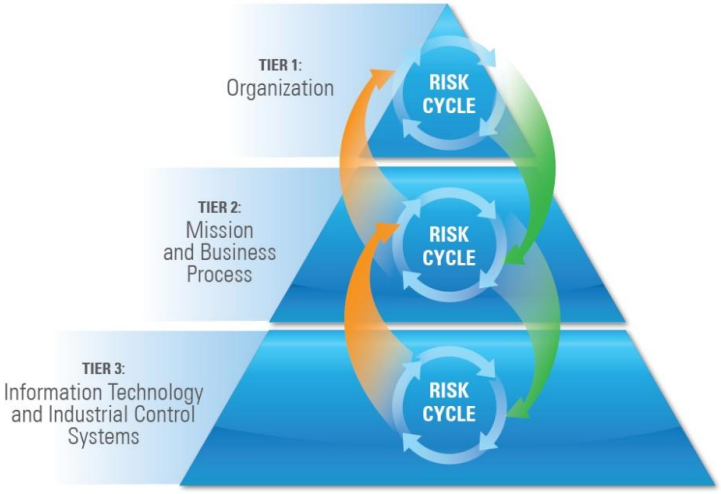
Risk Management Model

The risk management cycle is a continuous process for making risk decisions within each of the tiers defined in the risk management model. It is constantly re-informed by the changing risk landscape as well as changing organizational priorities and functions. The risk management cycle provides four elements that structure an organization's approach to risk management: frame; assess; respond; and monitor.



Risk Management Cycle

The RMP is based on integrating the risk management cycle at each business tier in the risk management model. The goals of this process are to improve risk-assessment, awareness, and security behavior at all levels of an organization. The process is designed to 1) accommodate any size or type of organization; 2) support a mission and business focused "top down" approach, and 3) support improved communication of risk across the organization.



Risk Management Process

The challenge to an electricity sector organization is to improve its awareness, monitor its risk, and improve its ability to survive potential cybersecurity events. This guide supports the maturation of a cybersecurity program and provides a means to improve communications, address change and support the business mission, operations, and executive management functions of the organization.

For Additional Information Contact:
Matthew Light
RMP Project Manager
matthew.light@hq.doe.gov